AC.JP における隠れオープンリゾルバの対策状況 2023

鈴木 常彦 [1)]

1) 中京大学 工学部

tss@suzuki.sist.chukyo-u.ac.jp

Status of Countermeasures against Hidden Open Resolvers in AC.JP

Tsunehiko Suzuki[1)]

1) Chukyo University

概要

隠れオープンリゾルバ (送信元詐称クエリが到達する DNS リゾルバ) の対策状況を追跡している。2011 年春から約 10 万のリゾルバを追跡調査している。JP では 3 割が脆弱であったがこれまでに対策されたのはその 36% である。2022 年 11 月の経営情報学会と 2023 年 2 月の電子情報通信学会で経過報告を行っているが本報告はその後の状況について特に AC.JP に関して報告するものである。AC.JP では最初の報告から 900 日を経過しても約 8 割が未対策である。

1 はじめに

2008 年 3 月の筆者によるオープンリゾルバの調査 [1] 以降、2008 年のキャッシュポイズニング騒動 [2][3] や 2013 年の DDoS 攻撃の流行 [4] などにより DNS のオープンリゾルバの対策は進んで来たが、同時に行うべき送信元詐称対策はあまり進んでいない。

ネットワーク境界で送信元詐称パケットの流入を許すと、許可された内部からのアクセスも偽装した攻撃が可能となり、サーバでのアクセス制限が意味を失う。これは DNS のみならず ICMP や NTP, SNMP, QUIC, SSDP, Memcached, LDAP 等々の UDP サービスへの攻撃や TCP への SYN flood 攻撃などに対しても、非公開のつもりのサーバが無防備となっていることを意味する。

2022 年 11 月に「減らない脆弱性 - 隠れオープンリゾルバ」[5] という研究発表を経営情報学会で行った。これは 2021 年 3 月からの調査によって送信元詐称対策が行われていないネットワークにあってサーバのアクセス制限が意味をなしていない DNS キャッシュサーバを多く発見した報告である。

また 2023 年 2 月には「隠れオープンリゾルバのスキャナー開発と調査 〜 進まない脆弱性対策 〜」[6] と題して電子情報通信学会でも対策状況を報告した。本報告はその後の状況について特に AC.JP に関して報告するものである。

2 日本の隠れオープンリゾルバの状況

約 10 万 IP アドレスをスキャンしている。調査開始時点の 2021 年 3 月 7 日に PTR の末尾が.JP. であるものを抽出して JPCERT/CC へ届けた。この時点での隠れオープンリゾルバは 300 ドメイン 736 IP アドレスであった。調査対象とした JP の IP アドレス数 2,462 の 3 割に相当する。その後、追加で発見されたものを加えた 774 IP アドレスを初期値として 2021 年 4 月 24 日から日毎の追跡調査を開始した。

対策の推移状況を以下の図 1 と表 1 で示す。表には脆弱なリゾルバの数とその 90 日毎の削減率と調査開始時点からの削減率を掲載する。

本調査には通常のオープンリゾルバも 1 割程度含まれている (2022 年 8 月 29 日時点で 40/588=7%) がソース IP アドレス詐称パケットが到達しておりネットワークの脆弱性が確認されているものである。

先の論文 [5] で示したとおり、2021 年 9 月 7 日に筆者のサイトにおいて脆弱なドメインの公開 [10] を行った際に約 1/4 が対策したものの、本論執筆の 2023 年 10 月においても 497/783、64% のサーバが未対策である。

3 AC.JP の隠れオープンリゾルバの調査

調査の方法を説明する。筆者の大学や国内のホスティング事業者の多くでは BCP38[11] 等の送信元 IP

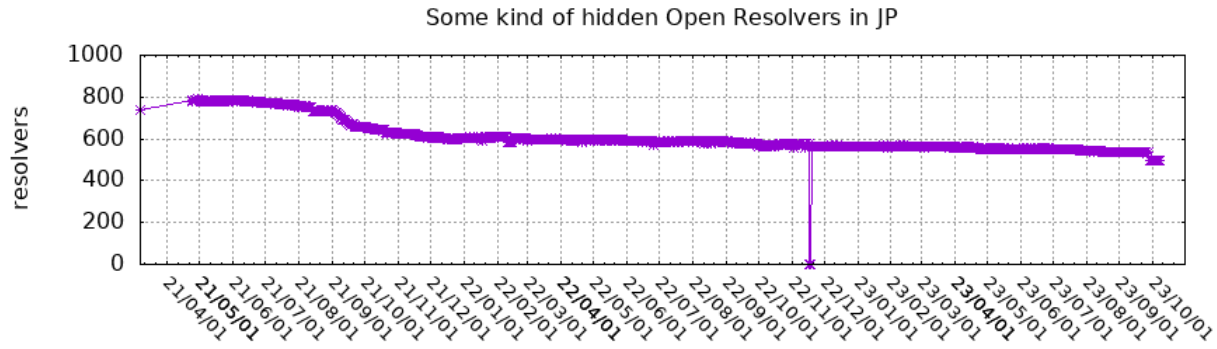

図 1　対策の推移 (JP)

表 1　対策の推移 (JP)

日付	脆弱数	90 日削減率	削減率	イベント
’21/04/24	783			追跡開始
’21/07/12	774			公開予告
’21/07/22	763	-2.6%	-3.4%	90 日後
’21/09/07	713			リスト公開
’21/10/20	628	-18%	-20%	180 日後
’22/01/16	609	-3%	-22%	270 日後
’22/04/16	595	-2.2%	-24%	360 日後
’22/07/15	586	-1.5%	-25%	450 日後
’22/10/13	565	-3.5%	-28%	540 日後
’23/01/11	563	-0%	-28%	630 日後
’23/04/11	558	-1%	-29%	720 日後
’23/07/10	550	-1.4%	-30%	810 日後
’23/10/08	497	-9.6%	-36%	900 日後

アドレスを詐称したパケットの送出防止対策が施されているため、欧州のホスティング業者のサーバ (VPS) を契約してスキャンを行っている。

AC.JP の継続調査においては以下の 3 種類の詐称 IP アドレスを送信元とした DNS クエリを用いている。

1. 対象のリゾルバに隣接する IP アドレス
2. 対象のリゾルバと同じ IP アドレス
3. 某ルートサーバの IPP アドレス

調査用クエリの問い合わせドメイン名は筆者の管理するドメイン名 reflec.to をサフィックスとした以下の様式のドメイン名である。

IP アドレス +”.”+ 詐称形式 + 日付 +”.acjp-scan.reflec.to”

例: 192.0.2.1.shift0901.acjpscan.reflec.to

詐称クエリが調査対象のリゾルバに届いて受け入れられると、当該リゾルバはその名前解決のためのクエリ (非再帰の反復問い合わせ) を筆者の管理する reflec.to の権威サーバへ送ってくる。その時点で当該のリゾルバは送信元詐称対策がなされていないネットワークで運用されている隠れオープンリゾルバであることが判明する。そのクエリログを毎日自動解析してデータの蓄積と公開 [16] を行っている。

4　文科省への報告

2021 年 9 月に 1,667 ドメインの AC.JP から AC.JP のホスト名のついた DNS 権威サーバを 1,132 台抽出して調査を行った。その結果、224 の AC.JP ドメインに 323 の隠れオープンリゾルバを発見した。これらのサーバは権威とキャッシュが同居していることも意味する。権威とキャッシュの同居の弊害については筆者のサイト「キャッシュサーバを権威サーバと兼用すると危ない」[17] を参照されたい。

調査結果は 2021 年 9 月 17 日に文部科学省の CSIRT (大臣官房政策課サイバーセキュリティ・情報化推進室) へ情報提供して対策への協力を求めた。

5　現在の状況

その後、継続調査を行っているが公開リスト [16] に示すようにおよそ 1 年後の 2022 年 9 月 3 日において約 9 割 (207 ドメイン、291 IP アドレス)、2023 年 10 月 8 日現在に至っても 1,085 のスキャン対象リスト中 189 ドメイン (当初の 224 ドメインに対して 84%), 264 IP アドレス (当初の 323 アドレスに対して 81%) が未対策で残存している。JP 全体が 36% 減ったのと比べると大学の対応は非常に鈍い。

なお高等専門学校 (*-nct.ac.jp, *-ct.ac.jp) は 2021 年 09 月 17 日の調査で 11 ドメイン, 17 IP アドレスが存在していたが、2023 年 5 月 15 日に 0 となった。これは独立行政法人国立高等専門学校機構が主導して対策が進められた結果だと聞いている。

6 対策

オープンリゾルバの対策はサーバ (リゾルバ) でアクセス制限するだけでは不十分である。境界ルータ (あるいはファイアウォール) の外側インターフェイスで内部 IP アドレスを詐称したパケットの流入を止める必要がある。これは DNS のみならずあらゆる送信元詐称攻撃を防ぐために重要なことである。

例えば内部のアドレスが 192.0.2.0/24 だった場合、FreeBSD の標準ファイアーウォール ipfw を例にとると

> deny all from 192.0.2.0/24 to any in via ${ 外側 IF}

というルールで止められる。

また自組織が外部への攻撃元にならないよう境界ルータの内側インターフェイスから内部 IP アドレス以外の流出を止めること (BCP38[11]) も重要である。

> deny all from not 192.0.2.0/24 to any in via ${ 内側 IF}

基本はネットワークでの対策になるが、ネットワーク管理者の協力が得られないサーバ管理者の自衛策として筆者は以下の対策を行っている。

> deny all from 192.0.2.0/24 to me not ipttl 64,128,255

これはルータを越えてくるパケットは IP TTL がカウントダウンしているが同一セグメントからのパケットは IP TTL が初期値のままであることを利用したものである。しばらくパケットを観察しそのネットワークで使用されている機器の IP TTL を収集すると良い。

扱う IP アドレスブロックの多いネットワークでの対策は難しくなるかもしれないが分割したネットワーク毎の対策やトポロジーの再設計、そして利用ポリシーの明確化で対策は進められるはずである。守るべきは DNS ばかりではない。

なお、自分の利用しているリゾルバが隠れオープンリゾルバかどうかは前述した Hidden Open Resolver Tester [18] で判定可能である。

7 まとめ

本研究は独自収集した約 10 万のリゾルバに対する調査ではあるが先の論文 [5],[6] と合わせ以下のことが判明している。

1. 隠れオープンリゾルバは 20% 存在する (調査対象 2,462 中 497)
2. 追跡調査開始からの 900 日後の現在で 64% が未対策
3. 1,085 のスキャン対象 AC.JP リスト中 189 ドメイン (当初の 224 ドメインに対して 84%), 264 IP アドレス (当初の 323 アドレスに対して 81%) が未対策

水責め攻撃の踏み台となって対外的にも害となる隠れオープンリゾルバ、そしてその原因となっているネットワークの送信元詐称に対する脆弱性は早急に対策を進めて頂きたい。

参考文献

[1] 鈴木常彦, オープンリゾルバの状況, 情報処理学会研究報告 (IPSJ SIG technical reports) 2008 (37), 89-91, 2008-05.

[2] B. Mueller,Improved DNS Spoofing Using Node Re-delegation, http://dl.packetstormsecurity.net/papers/attack/Whitepaper-DNS-node-redelegation.pdf, 参照 Feb. 1,2023.

[3] D. Kaminsky, It's the End of the Cache as We know it, https://www.slideshare.net/dakami/dmk-bo2-k8, 参照 Feb. 1,2023.

[4] JPCERT/CC,DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起, https://www.jpcert.or.jp/at/2013/at130022.html, 参照 Feb. 1,2023.

[5] 鈴木常彦, 減らない脆弱性 - 隠れオープンリゾルバ -, 経営情報学会 全国研究発表大会要旨集 2023 年 202211 巻 3D-6,2022

[6] 鈴木常彦, 隠れオープンリゾルバのスキャナー開発と調査 〜 進まない脆弱性対策 〜, 電子情報通信学会 NS 研究会, 信学技報, vol. 122, No. 406, NS2022-229, pp.357-361,2023

[7] JPRS,DNS リフレクター攻撃（DNS アンプ攻撃）,https://jprs.jp/glossary/index.php?ID=0156, 参照 Feb. 1,2023.

[8] JPRS, ランダムサブドメイン攻撃（DNS 水責め攻撃）, https://jprs.jp/glossary/index.php?ID=0137, 参照 Feb. 1,2023.

[9] Yuuki Takano and Ruo Ando and Satoshi Uda andc Takeshi Takahashi and Tomoya Inoue,The Ecology of DNS Open Resolvers,ICECE Transaction B, Vol. J97-B, pp. 873-889, 2014.

[10] 鈴木常彦, 隠れオープンリゾルバを放置している日本のドメイン, https://snoopy.e-ontap.com/vulnerables.html, 参照 Feb. 1,2023.

[11] P. Ferguson,D. Senie,RFC2827(BCP38) Ingress Filtering,
IETF, https://www.rfc-editor.org/rfc/rfc2827.html, 参照 Feb. 1,2023.

[12] E. Dobelis,kamene, https://github.com/phaethon/kamene, 参照 Feb. 1,2023.

[13] 鈴木常彦, 隠れオープンリゾルバ, http://www.e-ontap.com/dns/hidden-openresolver/, 参照 Feb. 1,2023.

[14] 鈴木常彦,Port Randomize Tester, http://www.e-ontap.com/blog/20111114.html, 参照 Feb. 1,2023.

[15] 鈴木常彦,(隠れ) オープンリゾルバとなっていた謎のアプライアンスが機能停止, http://www.e-ontap.com/blog/?date=20220521, 参照 Feb. 1,2023.

[16] 鈴木常彦, 隠れオープンリゾルバを放置している AC.JP, http://www.e-ontap.com/dns/hidden-openresolver/, 参照 Feb. 1,2023.

[17] 鈴木常彦, キャッシュサーバを権威サーバと兼用すると危ない, http://www.e-ontap.com/dns/weirdra/, 参照 Oct. 8,2023.

[18] 鈴木常彦,Hidden Open Resolver Tester, https://snoopy.e-ontap.com/

[19] M. Korczyński,et al., Don't Forget to Lock the Front Door! Inferring the Deployment of Source Address Validation of Inbound Traffic, International Conference on Passive and Active Network Measurement, Mar 2020, Eugene, United States., https://mkorczynski.com/PAM2020Korczynski.pdf,

[20] The Closed Resolver Project, https://closedresolver.korlabs.io/, 参照 Feb. 1,2023

[21] CAIDA. 2020. The Spoofer Project, https://www.caida.org/projects/, 参照 Feb. 1,2023.

[22] 大井, 落合, 江崎, オープン DNS リゾルバの現状把握手法の提案と評価, マルチメディア，分散協調とモバイルシンポジウム 2018 論文集, 2018, 1126-1133, 2018-06-27.

[23] 脆弱性関連情報に関する取扱規程, 経済産業省, https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf, 参照 Feb. 1,2023.

[24] IPA, 情報セキュリティ早期警戒パートナーシップガイドライン,IPA, https://www.ipa.go.jp/files/000098799.pdf, 参照 Feb. 1,2023.

[25] 脆弱性関連情報取扱いガイドライン,JPCERT/CC, https://www.jpcert.or.jp/vh/vul-guideline2017.pdf, 参照 Feb. 1,2023.